Spring 2019

NORTHERN ARIZONA UNIVERSITY | College of Engineering, Forestry, and Natural Sciences

School of Informatics, Computing, and Cyber Systems

INF 639

General Information

- *Course title*: Nanomaterials and Nanoelectronics for Cybersecurity
- *Semester/Section*: Spring 2019
- *Credit hours*: 3
- *Meeting time and location*: Thusdays 5:30-8pm, SICCS building, room 103
- *Instructor*: Bertrand Cambou
  - *Instructor email*: bertrand.cambou@nau.edu
  - *Office location*: 110
  - *Office hours*: Open – call 408 203 1648 when absent

Course Prerequisites

Graduate status.

Academic Catalog Description

Study of methods, techniques, and research areas in nanomaterials and nanoelectronics to strengthen cybersecurity.

Course Purpose

This project-based course is intended to provide a graduate-level study of using nanotechnology in strengthening hardware applications in cybersecurity, including applications in the Internet of Things and government asset protection, and is particularly appropriate as an elective for students in the MSEE and PHDINF programs. The main objective of the course is to present how nanomaterials, and nanoelectronics can strengthen cyber physical systems (CPS) through hardware authentication, leveraging lectures, in-class discussion, in-class assignments, homework assignments, scholarly literature reading assignments, and a multi-part development project. The course will start with a general overview of the importance of hardware based security for CPS, and example of use of nanotechnologies. Elements of nanoelectronics will be presented, physics of important components (MOSFET, SRAM cell, DRAM cell, Flash cell, Resistive RAM cells, MEMS, and Sensors), and the importance of nanomaterials. Continuing, the course will cover the design and use of secure elements and their related security limitations under side-channel attacks as well as authentication methods, including biometrics and physically unclonable functions (PUF). The design of True Random Number Generators from nanoelectronics devices will be presented. The course will conclude with the use of traditional microelectronic components and how nanotechnologies can be leveraged in resolving fundamental weaknesses in combination with embedded software and encryption methods. By the end of the course, students are able to engage in research applications of nanotechnologies in cybersecurity and apply the principles of cybersecurity in a variety of applications in other research areas of interest in computer science, electrical engineering, and informatics.

Student Learning Outcomes

Upon successful completion of this course, students will be able to demonstrate the following advanced competencies:

- Analyze, evaluate, and articulate the general uses of authentication methods, and nanomaterials and nanoelectronics in strengthening cybersecurity and responding to hacking attacks;
- Evaluate, select nanoelectronics components, authentication methods, and nanotechnology architectures, and embedded software techniques to the design and development of cybersecurity solutions to a variety of application domains;
- Apply nanotechnologies to the design, implementation, and assessment of novel secure elements architectures using hardware authentication, physically unclonable functions, and true random number generators;
- Identify, interpret, and critically explain the significance of open research areas and questions in the design of hardware devices in cybersecurity.

Course Structure

This offering of INF 639 will consist of lectures, in-class assignments, homework assignments, scholarly literature reading assignments, and a multi-part development project.

Textbook and Required Materials
"Nanoelectronics and Information Technology, advanced Electronic Materials and Novel Devices" by Rainer Waser (Editors) – Wiley-VCH (ISBN 978-3-527-40927-3).

Recommended Materials and Readings
Additional readings will be provided from various sources, including:

- *"Semiconductor Device Fundamentals"* by Robert F. Pierret – Pearson (ISBN: 978-81-775-8977-1).
- *"Microelectronic circuits"* by Sedra/smith (ISBN: 0199339139).

Course Outline
For a more detailed outline, check the course schedule. Topics will include: introduction to nanomaterials and nanoelectronics research areas to strengthen CPS; specific cryptographic methods: physically unclonable functions, authentication and multi-authentication methods, multi-key management; attacks and hacking techniques with defensive methods, including side-channel attacks and true random number secure elements; use of nanotechnologies in secure elements and secure embedded memories; designing secure state machines; novel nanotechnologies and benefits for cybersecurity; statistical approaches to validating nanotechnology manufacturing techniques; secure system integration: embedded software and operating system techniques and partitioning functions in hardware and software. Breaches in cybersecurity are often due to solutions build on silos, the understanding of the connected disciplines is essentials. This class encourage inter-discipline partnership, and team work. The agenda covered during the semester should be similar than the following (weekly schedules are approximate, and subject to minor changes):

1. From Micro to Nano-electronics (week 1)
2. Introduction to cryptography (week 1)
3. Public Key Infrastructure (week 2)
4. Smartcards (week 3)
5. Attacks on smartcards (week 4)
6. MOS transistor & logic circuits (week 5 to 6)
7. Biometry (week 7)
8. Physical Unclonable Functions (PUF) (week 8 to 9)
9. Access control and authentication (week 10)
10. Flash Memory devices & security (week 11)
11. Resistive RAM & security (week 12)
12. Sensor devices and security (week 13)
13. Public key cryptography (week 13 to week 14)
14. Research in Ternary cryptography (week 15 if time permits)

Assessment of Student Learning Outcomes
Methods of assessment include: In-class and reading assignments assess expertise in articulating and evaluating the use of nanoelectronics in authentication; homework assignments assess student ability to apply nanotechnologies to the design of systems; and a multi-stage research project assesses the ability to identify, interpret, and explain open research questions in cryptography as well as the ability to design and apply solutions using hardware devices to develop secure systems.

Grading System
The weight of each course component toward your final grade is:

Assignment	Grade Weight %
Attendance (no miss: 100% - 10 hours miss or more: 0%)	15%
In class assignments (Very active: 100% - passive: 0%)	15%
Homework assignments (To be presented within two working weeks)	15%
Research project #1: Demonstrate understanding of the basic concepts	15%
Research project #2: Demonstrate understanding of the advanced concepts	15%
Research project #3: Demonstrate ability to implement and generalize	15%
Research projects: additional final report	10%

Homework:
The students will have the opportunity to prepare 1-2 homework by session of 2&1/2 hrs. The objectives of the homework are to summarize, and practice elements directly related to the class. This could be some mathematical computations, detailing examples presented in class, or finding additional examples similar than the ones presented. The students are not required to prepare all suggested homework, quality is preferred to quantity. A good student should try to prepare at least 75% of the proposed homework.

Projects:
A project assesses the student ability to select, describe, synthesize and present material related to what is presented in class on a topic of their choice. Examples of successful projects include the programing of a javacard to encrypt small message, or a development of small circuitry demonstrating the functionality of physical unclonable functions. The students will be encouraged to present their projects in class, and to prepare small tutorials explaining the context, and bigger picture, of their projects. If they cannot present all three projects in class, the students will have the opportunity to do so during office hours. One of the project can also be a written document submitted at least 5 days before the end of the semester. On demand, and when relevant, the students will have access to the cybersecurity lab to work on their projects. The students will have the latitude to pick a project in line with their general area of expertise, and to partner with one to three peers. If the students wish to present group projects, they need to have different partners for each project. The outcome could be a combination of small electronic systems, some programming work, and literature work demonstrating their understanding (project#1 &2), and mastering of the subject (project#3).

Grades will be awarded on the following scale:

Percentage Grade	**Letter Grade**
90% or above	A
80% through 89%	B
70% through 79%	C
60% through 69%	D
59% or below	F

There is no "curve;" your grade is completely up to you and is not affected by the grades of your classmates. Extra credit opportunities may present themselves throughout the semester and be announced during class meetings. If you feel a mistake has been made in grading your assignment, please address your concerns during office hours.

NORTHERN ARIZONA UNIVERSITY
POLICY STATEMENTS FOR COURSE SYLLABI
HTTP://NAU.EDU/CURRICULUM-AND-ASSESSMENT/_FORMS/CURRICULAR-POLICY/SYLLABUS_POLICY_STATEMENTS/